FIPS PUB 87

FEDERAL INFORMATION
PROCESSING STANDARDS PUBLICATION

1981 MARCH 27

U.S. DEPARTMENT OF COMMERCE / National Bureau of Standards

GUIDELINES FOR ADP CONTINGENCY PLANNING

CATEGORY: ADP OPERATIONS

SUBCATEGORY: COMPUTER SECURITY

U.S. DEPARTMENT OF COMMERCE, Malcolm Baldrige, *Secretary*
NATIONAL BUREAU OF STANDARDS, Ernest Ambler, *Director*

Foreword

The Federal Information Processing Standards Publication Series of the National Bureau of Standards is the official medium for promulgating standards under the provisions of Public Law 89-306 (Brooks Act) and under Part 6 of Title 15, Code of Federal Regulations. These legislative and executive mandates have given the Secretary of Commerce important responsibilities for improving the utilization and management of computers and automatic data processing (ADP) systems in the Federal Government. To carry out the Secretary's responsibilities, the NBS, through its Institute for Computer Sciences and Technology, provides leadership, technical guidance and coordination of Government efforts in the development of guidelines and standards in these areas.

These guidelines were developed, as part of the security and risk management program, to provide technical and managerial guidance to Federal agencies that will further the protection of vital ADP resources. Contingency planning is an integral part of the program for any data processing operation, for without a tested and effective plan to respond to and recover from unexpected and sudden disruptions of service, minor problems may become major and major problems may become catastrophic. Although a contingency plan will not prevent a natural disaster such as a flood, tornado, and the like, it will mitigate the effects of such unfortunate occurrences. It is often thought that contingency plans are designed only for major disasters; however, empirical evidence indicates that, ordinarily, the most serious threats to ADP resources are the more mundane happenings such as accidental destruction of data through human error, water damage due to burst water pipes, etc. Preparation of a contingency plan gives managers an excellent opportunity to alleviate or minimize potential problems which would disrupt data processing service. If, during development of a contingency plan, critical systems are identified and documented, a systematic method of emergency response is developed and backup operations procedures and recovery planning are accomplished, the future well-being of the ADP operation will most assuredly be enhanced. NBS is pleased to make these Guidelines for ADP Contingency Planning available for use by Federal agencies.

James H. Burrows, *Director*
Institute for Computer Sciences
and Technology

Abstract

This document provides guidelines to be used in the preparation of ADP contingency plans. The objective is to ensure that ADP personnel, and others who may be involved in the planning process, are aware of the types of information which should be included in such plans; to provide a recommended structure and a suggested format; and generally to make those responsible aware of the criticality of the contingency planning process.

Key words: ADP availability; ADP security; backup operations; computer applications; computer security; contingency planning; emergency response; Federal Information Processing Standards Publication; recovery actions.

Nat. Bur. Stand. (U.S.), Fed. Info. Process. Stand. Publ. (FIPS PUB) 87, 31 pages.
(1981)
CODEN:FIPPAT

For sale by the National Technical Information Service, U.S. Department of Commerce, Springfield, VA 22161.

Federal Information Processing Standards Publication 87

1981 March 27

ANNOUNCING THE

GUIDELINES FOR ADP CONTINGENCY PLANNING

Federal Information Processing Standards Publications are issued by the National Bureau of Standards pursuant to the Federal Property and Administrative Services Act of 1949 as amended, Public Law 89-306 (79 Stat. 1127), and as implemented by Executive Order 11717 (38 FR 12315, dated May 11, 1973), and Part 6 of Title 15 Code of Federal Regulations (CFR).

Name of Guideline: Guidelines for ADP Contingency Planning.

Category of Guideline: ADP Operations, Computer Security.

Explanation: These guidelines describe for organizational and data processing management, and for managers who obtain data processing services from other activities, what should be considered when developing a contingency plan for an ADP facility. They also provide a suggested structure and format which may be used as a starting point from which to design a plan to fit each specific operation.

Approving Authority: U.S. Department of Commerce, National Bureau of Standards (Institute for Computer Sciences and Technology).

Maintenance Agency: U.S. Department of Commerce, National Bureau of Standards (Institute for Computer Sciences and Technology).

Cross Index:

a. Federal Information Processing Standards Publication (FIPS PUB) 31, Guidelines for Automatic Data Processing Physical Security and Risk Management.
b. Federal Information Processing Standards Publication (FIPS PUB) 38, Guidelines for Documentation of Computer Programs and Automated Data Systems.
c. Federal Information Processing Standards Publication (FIPS PUB) 39, Glossary for Computer Systems Security.
d. Federal Information Processing Standards Publication (FIPS PUB) 41, Computer Security Guidelines for Implementing the Privacy Act of 1974.
e. Federal Information Processing Standards Publication (FIPS PUB) 46, Data Encryption Standard.
f. Federal Information Processing Standards Publication (FIPS PUB) 48, Guidelines on Evaluation of Techniques for Automated Personal Identification.
g. Federal Information Processing Standards Publication (FIPS PUB) 64, Guidelines for Documentation of Computer Programs and Automated Data Systems for the Initiation Phase.
h. Federal Information Processing Standards Publication (FIPS PUB) 65, Guideline for Automatic Data Processing Risk Analysis.
i. Federal Information Processing Standards Publication (FIPS PUB) 73, Guidelines for Security of Computer Applications.
j. Federal Information Processing Standards Publication (FIPS PUB) 76, Guideline for Planning and Using a Data Dictionary System.
k. Federal Information Processing Standards Publication (FIPS PUB) 77, Guideline for Planning and Management of Database Applications.

Applicability: These guidelines are applicable to all Federal agencies required to take action under the Office of Management and Budget Circular A-71, Transmittal Memorandum No. 1 of July 27, 1978, to ensure the development of appropriate contingency plans.

Implementation: These guidelines should be referenced in the formulation of contingency plans by Federal agencies for ADP facilities whether operated directly by Federal agencies or under contract.

Specifications: Federal Information Processing Standards Publication (FIPS PUB) 87, Guidelines for ADP Contingency Planning (affixed).

Qualifications: These guidelines have been prepared to provide management personnel with information on which workable, usable contingency plans for ADP facilities can be developed and implemented. These guidelines are not all inclusive, and do not suggest that there is but one method of devising contingency plans. There are, indeed, many possibilities and scenarios which management might follow; however, when used, these guidelines spare management the necessity of devoting the time and effort of determining alternate methods, and will permit them to expend their resources productively in the development and testing of the plan and procedures, thus hopefully preparing themselves for contingency operations. Most importantly, careful execution of these procedures will invariably highlight potential problems and give management an opportunity to preclude many of those incidents which would require actual implementation of the plan.

Where to Obtain Copies of these Guidelines: Copies of this publication are for sale by the National Technical Information Service, U.S. Department of Commerce, Springfield, VA 22161. When ordering, refer to Federal Information Processing Standards Publication 87 (FIPS-PUB-87) and title. When microfiche is desired, this should be specified. Payment may be made by check, money order, or deposit account.

Federal Information
Processing Standards Publication 87

1981 March 27

Specifications for

GUIDELINES FOR ADP CONTINGENCY PLANNING

CONTENTS

1. INTRODUCTION

The continued growth in dependence on computers and on the data processed by them has increased the importance of plans to prevent loss of their availability. Only a few years ago it was reasonable to consider recourse to manual operations when automatic data processing (ADP) systems became unavailable. Today, there are but few situations in which it is even possible to revert to manual processes. Thus, contingency plans are necessary to minimize the damage caused by unexpected and undesirable occurrences (contingencies) in and about the ADP facilities.

Security measures are employed to prevent or detect accidental or intentional disclosure, modification, or destruction of data or loss of the means of processing those data. Contingency plans, on the other hand, should be designed to reduce to an acceptable level the consequences of any loss of ADP resources or capability; they are not just planned responses to major catastrophes. As stated earlier, the purpose of a contingency plan is to mitigate the damaging consequences of unexpected and undesirable events *of whatever magnitude.* A contingency plan must not be directed exclusively at reaction to catastrophically destructive occurrences. While it is clearly true that those who are responsible for ADP resources must plan for the possibility of such catastrophic loss, they must also plan against less-than-cataclysmic events which also seriously impede provision of data processing functions.

The probability of the occurrence of an undesirable event is generally inversely related to its magnitude. Usually, the greater the catastrophe, the lower the probability that it will happen. In other words, data processing operations are disrupted with far higher frequency by small problems than by large ones.

There is another relationship which, while not obvious, is quite important to the quality of contingency plans. The size or scope of a catastrophe and of its effect on data processing operations are often not directly related. In the absence of a good plan, minor damage can cause major problems. Conversely, with a good plan, even major damage may not result in serious losses.

The following pages describe an orderly process for the generation of contingency plans. This document, however, is not intended to be an all inclusive source of information on contingency planning. Other sources such as FIPS Publication 31, Guidelines for Automatic Data Processing Physical Security and Risk Management [20], and others listed in section 5 should be used as appropriate to obtain additional data and ideas which may be applied when preparing the plan for any particular facility. The procedure in this document is provided to save those charged with the preparation of such plans the task of discovering or devising yet another process for doing so.

While this document is addressed primarily to data processing management, the information in it is also relevant to those organizations which do not operate a data processing center, but obtain support from other agencies or service bureaus through interagency or contractual agreements. Agencies receiving this type of data processing support should not assume that the servicing activities have adequately provided for any type of contingency. Thus, this document may be used to assist in establishing the requirements for adequate support during contingencies and in reviewing any applicable contingency plans for such organizations. Further, this document can also assist those users in a distributed data processing (DDP) network who operate or are responsible for equipment. Managers of such DDP activities should also consider contingency planning for their operation, and how the operation fits into the overall contingency plan for the entire network.

Few ADP operations and facilities are so similar in equipment configuration, applications, environment, personnel situation (particularly), and relative criticality of systems that a general-purpose contingency plan of broad applicability can be drawn and applied equally well to more than one facility. For this reason, no

recommended plan is provided here. Instead, a guideline is provided for preparing a specific plan suitable to the peculiar needs of each ADP facility. However, the contingency plan for any data processing activity, regardless of its size or scope of operation should, as a mimimum, address the following three elements:

- **Emergency Response**—Emergency response procedures to cover the appropriate emergency response to a fire, flood, civil disorder, natural disaster, bomb threat, or any other incident or activity, to protect lives, limit damage, and minimize the impact on data processing operations.

- **Backup Operations**—Backup operations procedures to ensure that essential data processing operational tasks can be conducted after disruption to the primary data processing facility. (Arrangements should be made for a backup capability, including the needed files, programs, paper stocks and preprinted forms, etc., to operate the essential systems/functions in the event of a total failure.)

- **Recovery Actions**—Recovery actions procedures to facilitate the rapid restoration of a data processing facility following physical destruction, major damage, or loss of data.

To the extent possible, contingency plan documents should be brief so as to facilitate their usefulness and acceptance by the users. The plan should be tested on a recurring basis and modified as changes in the data processing facility workload dictate. Critical applications should be operated on the backup system regularly to ensure that it can properly process this workload. (See sec. 4, Testing.)

2. ROLE OF MANAGEMENT

ADP facilities generally provide a service to one or more functional areas of organizations of which they are a part. Occasionally, they provide data processing support to several organizations. Recognition that the ADP shop serves in a support role is essential to the proper conduct of many aspects of data processing management. It is no less important to the generation of realistic, cost-efficient contingency plans.

Because the ADP facility normally provides vital services to the organization, the senior management of each organization should realize the critical nature of that organization's dependence on contingency plans. These plans, if carefully prepared and executed, serve to keep within tolerable limits the consequences of losses or damage to ADP resources. Economic feasibility in contingency plans requires carefully derived decisions as to what organizational functions are deferrable and for how long. As described later, the costs of these deferrals should be established.

It is practically impossible for such decisions to be reached entirely within the ADP organization. The ADP management is not usually in a position to assess accurately the relative importance to the whole organization of work done by the respective supported areas. Further, the relative cost of continued support of each in the face of adversity may vary quite widely. Thus, cost of support under unusual conditions must be considered. For these reasons, it is not only appropriate but very important that the senior agency management provide direction and support for contingency planning to the end that the agency continue to provide essential services following disruption of the ADP facility. Senior management should do the following:

- Demonstrate a firm commitment to the ADP security program by promulgating objectives and including responsibilities to attain those objectives in job descriptions and in promotion plans, when appropriate.

- Direct the establishment of contingency plans which are based on the results of a comprehensive risk analysis.

- Direct the support of the planning process by all organizational units servicing and serviced by the ADP facility. In particular, identify those elements of the organization which are critically dependent upon the ADP facility. Of extreme importance is the assistance of supported activities in identifying those vital records and data maintained by the ADP function, i.e., those which are essential to the sustained continuation of supported activities following a disruption of service or destruction of the ADP facility. (Responsibility for preparation of the plan should be with the ADP facility.)

- Direct the initial and periodic later tests of the workability and costs associated with the plan. (See sec. 4, Testing.)

- Direct the periodic revision or update of the plan as a consequence of information derived from the tests, and as a result of changing dependence of the organization on ADP. Likewise, a complete review of the plans should be made upon addition of new applications systems, reaccomplishment of a risk analysis or a change in any of the critical dependencies.

2.1 Risk Analysis

The development of a contingency plan to minimize the damage resulting from losses or damages to the resources, or capability of an ADP facility is dependent for its success on recognition of the potential consequences of undesirable events against which the facility needs protection. The facility is an assemblage of many resources. Some particular subset of these is needed by the facility to provide data processing support. These resources include people, programs, data, data processing hardware, communications facilities, power, environmental control, the physical facility and access to it, and even paper forms.

All resources are not equally important. They are also not equally susceptible to harm. Therefore, the selection of safeguards, and the elements of a contingency plan, should be done with informed awareness of which system functions are supported by each resource element (devices, programs, data, etc.), of the susceptibility of each element to harm (accidental or intentional), and of the consequences of such harm. In short, cost-effective protection of a data processing facility is heavily dependent on:

- An awareness of the facility's relative dependence on each of its component parts,

- Knowing, at least, in an overall way, what the chances are that something undesired will happen to each component,

- A determination of the ramifications of undesired things happening so that, things can be done to minimize either the chances of their happening, the loss if they happen, or both.

The maximum allowable cost of any safeguard is limited by the size of the expected losses which will be mitigated by that safeguard. Any safeguard or combination of safeguards must not cost more than tolerating the problems to which the safeguards are addressed. Satisfaction of these criteria clearly requires a process which identifies the expected losses as a consequence of undesired things happening to resources. Such a process is called a risk analysis.

In addition to providing a basis for the selection and cost-justification of security measures, a risk analysis provides data on time as a factor in assessing the possible consequences of losses of security. Knowledge of the consequences of not being able to perform each system function for specific time intervals is essential to the

creation of contingency plans which are adequately responsive to the needs of the supported organizations.

With very few exceptions, a large percentage of an ADP facility's workload is deferrable for significantly long periods of time before the deferral causes unacceptable hardship. On the other hand, there is usually a small percentage of the workload which must be run because its delay would cause intolerable disruption. It has proven very difficult to guess reliably and accurately into which category each data processing activity should fall. It is also very difficult to guess very accurately the maximum tolerable delay for the processing of each deferred activity. A properly conducted risk analysis yields these data, which can then be used to justify or reject contingency plan elements based on actual, quantitatively-expressed needs of the supported organizations for ADP services.

A suggested risk analysis procedure which provides the desired data is described in FIPS Publication 65, Guideline for Automatic Data Processing Risk Analysis [22].

2.2 Critical Dependencies

As described earlier, the prompt recovery of an ADP facility from a loss of capability is dependent upon the availability of a variety of resources. The specific resources required are a function of the nature of the problem which generated the need for recovery. Some of these resources are absolutely essential to reestablishment of operations and, as such, are critical dependencies which warrant special care to assure their continuing availability and early recognition of a loss of capability. These things on which there is a critical dependence are usually in two distinct categories, which are:

- Resources under the direct control of the ADP management.

  Within this category special care must be placed on determining which data are needed for backup and recovery purposes. There is generally a certain amount of information which is absolutely vital to the organization, and which would have the first priority in any emergency situation. This information must be identified very clearly to facilitate its availability. There exists also in any ADP facility much remaining data which are extremely useful to an organization, and which if they had to be regenerated could be very costly. This type of data should also be properly categorized and maintained. During a long term backup operation, it is quite normal for management to expect continued availability of many of the day-to-day ADP products and services. Obviously, if backup copies of the information are not routinely prepared and maintained, it will not be possible to provide acceptable service during backup and recovery situations.

- Resources under the control of other persons.

  The data processing management can and should take the steps necessary to assure the continuing availability of resources currently under its direct control. More difficult, but no less important, is the acquisition of firm commitment to the contingency plan of those resources under the control of persons outside of the data processing area. The external commitments of critical resources must be reviewed frequently to see that they have not been forgotten or otherwise neglected by the organizations making those commitments. Rehearsals or tests are the most satisfactory way of assuring the adequacy of most such commitments of critical resources.

After disruption of processing at the regular location, it is rarely logistically, technically or economically feasible, and even more rarely essential to continue all normal activity at the alternate location. The tasks performed by the facility are not all of equal importance. Further, the relative importance of many ADP systems may

vary with time of day and day of week or month. A plan which attempts to provide the means to continue all processing without regard to relative importance will require expensive standby capabilities which must be frequently exercised to assure availability and compatibility with normal activities. This is very rarely feasible and usually unnecessary.

2.3 Management Review and Approval

The review and approval process for a contingency plan should be carefully established to satisfy several important objectives, as follows:

- Make senior management aware of any dependencies upon it for supportive action. Ensure that management realizes that during an emergency, there may be some services which will not be provided, or otherwise available.
- Obtain management agreement on the assumptions on which the plan is based, including the dependence on other organizations for assistance.
- Communicate to management the existence of a plan and obtain approval of the plan.
- Obtain formal concurrence of certain other organizations upon which there might be dependence.
- Through required reading and acknowledgment by signature (usually on a separate card), inform key employees of their respective roles in the various recovery scenarios.

3. THE ADP CONTINGENCY PLAN

A reasonable, systematic approach to contingency planning and documentation of the plan demands adherence to a carefully conceived structure. This structure is needed to:

- Assure that all important areas are addressed,
- Permit ease of reference to sections of immediate interest or concern, and
- Facilitate revision by minimizing the effect on the whole document of changes in limited areas of concern. Therefore, unless there is very solid justification for doing otherwise, the documented plan should be in loose-leaf form, highly sectionalized, with each page numbered and dated and with means provided to identify changes from the previous version of each page.

A contingency plan should consist of three parts which address two distinct, mutually exclusive sets of activity:

- Preparation Phase
  - — Part One, Preliminary Planning
  - — Part Two, Preparatory Actions

These two parts should cover those things which should be or have been done in anticipation of a loss to lessen the damage or assist recovery.

- Action Phase
  - — Part Three, Action Plan

This part should cover those things which must be done after the fact to minimize the cost and disruption to the supported organizational functions.

Each part of the plan is essential to its overall workability and effectiveness; therefore, no part should be considered more important than another. There are differences, however, in the manner of their presentation.

Part One, Preliminary Planning, which is the basic driver of actions to take in the succeeding parts should be completed prior to beginning the actual preparation of the remaining parts of the plan.

Part Two, Preparatory Actions, describes specific preparation steps in a number of areas relevant to the facility and should be developed in as much detail as seems potentially beneficial. Such material can consist of "how to" instructions, and lists of information to the extent necessary. There will be time to read this material, to become educated in the problems and their potential solutions, to weigh alternatives and to select appropriate measures. An essential element of this part of the plan is unwavering insistence that *all persons on whom there is significant dependence during contingency operations be familiar with their potential respective roles*, i.e., when implementing Part Three of the plan. These persons are selected because they already know "how to." The plan must not be based on the assumption that the document describing it can be retrieved after the catastrophe by those with a role in recovery who will then read the plan to learn how to do what is needed of them. Except for supporting data from Part Two (such as lists of people, telephone numbers, addresses, and skills, of locations of things, of required resources to support key functions, and the like, i.e., things that are generally tabular in nature and difficult if not impossible to memorize), it should not be necessary to read the plan to initiate contingency operations.

Part Three, Action Plan, should consist of clearly stated actions which are to be taken upon the occurrence of an emergency. Part Three is divided into three sections: Emergency Response, Backup Operations, and Recovery Actions. Each of the three sections includes those things which are to be done in response to a set of problem scenarios. These problem scenarios are derived in a large part from information in the risk analysis process and from practical working experience. They must be representative of the reasonable anticipated problems. Immediately following each problem statement or scenario should be a description of what is to be done in each category described (not how). One scenario may require actions, and be listed, in one or more sections of this part, e.g., a bomb threat (which does not result in any damage), minor power outages, etc., may necessitate action only under Section One, Emergency Response. A sustained power outage would involve action under Section One and Section Two, Backup Operations. An incident causing serious damage to the facility would, most likely, require steps under Sections One, Two, and Three, Recovery Actions. Examples of typical scenarios and sections of the plan which might apply include:

- Sections One and Two. Fire or structural damage elsewhere in the building resulting in no loss of life has resulted in denial of access to the data processing facility for three days. Return to the ADP facility after that period is anticipated, but it might be slightly longer.

- Sections Two and Three. Destruction of the facility with loss of all personnel working at that time.

- Sections One, Two, and Three. Total communications failure.

- Sections One, Two, and Three. A hurricane, earthquake, tornado, or other natural disaster occurs which cripples local transport, power and communications but does little physical damage to the facility.

The scenarios mentioned above are not necessarily appropriate to any particular facility. The ones which are must be selected and be sufficiently large in number and breadth that they offer useful guidance in directing recovery in actual loss situations and in the performance of tests and rehearsals.

3.1 Plan Structure and Contents

A recommended structure for the ADP facility Contingency Plan is shown in the succeeding instructions, and includes suggested topics and information for each part and section of the plan. (An example Plan Outline is included as Appendix One.) While no one format can be totally appropriate for all situations and facilities, the plan structure as suggested here should be readily adaptable to virtually all ADP activities, regardless of the size or scope of operation. An essential point to remember while developing a contingency plan is that it should be viewed as a valuable, useful tool for the ADP facility and not as an additional burden which somehow must be borne.

3.2 Part One—Preliminary Planning

This part of the plan should describe the purpose, scope, assumptions, responsibilities, and overall strategy relative to the plan. Misconceptions concerning these concepts are quite common and must be clearly addressed to ensure that they are communicated to those who must effectively respond to a contingency by implementing the plan. This part should conclude with a section which provides for recording changes to the plan. Each section of Part One and recommended contents are described below.

3.2.1 Purpose

This section should describe the reason and objective for having a contingency plan. If, for example, the continued well being of the data processing facility's parent organization is heavily dependent upon the data processing facility, it would be entirely fitting in this section to convince the reader, i.e., user of the plan, that the plan is not prepared merely to fill some arbitrary square in a checklist, but that the plan documents actions which are mandatory, essential and which must be subjected to continual review and testing to assure their adequacy in case of a contingency. A lackadaisical approach to contingency planning, if inferred or somehow communicated to the reader in this section, will set the stage for a corresponding less-than-enthusiastic acceptance of the plan and its requirements by the employees. The statement of purpose should convey the notion that the plan is a dynamic, on-going activity which includes not just things which are done in anticipation of a problem; that is, things done before the fact to mitigate the damage and to ease recovery, but also what is to be done when problems occur.

3.2.2 Scope

This section should describe in concise terms the extent of coverage of the plan, e.g., "This plan is applicable to the data processing facility located in building 1234. It includes all functions, i.e., data processing and ancillary services, administrative functions, etc., associated with the Data Processing Division. It also includes off-site storage facilities located at (location)." It is especially important for large activities with multiple data centers, communications facilities, etc., to clearly state in this section whether the plan encompasses all facilities even though not co-located, or applies to just specific locations as mentioned. The existence and location of plans for other facilities, if applicable, could be referenced in this section to facilitate their retrieval when needed.

3.2.3 Assumptions

A contingency plan is based on several categories of assumptions. Most can be established only after a quantitative risk analysis. The whole list of assumptions for inclusion in the document cannot be completed until well along in the planning cycle. Included in the set of assumptions should be the following:

a. Nature of the Problem

— The general nature and range of events against which the plan is directed.

— Events not addressed by the plan which, because of their low probability, do not warrant consideration in the plan.

— Events which are so extensive in scope as to negate the feasibility for early recovery of data processing operations.

— Events too minor in scope to warrant reflection in the plan. These are generally sufficiently frequent as to be considered a normal part of the operation and which are now accommodated routinely.

b. Priorities

Senior organization and ADP management have a critical need to understand the manner in which priorities are determined. The data sources, the extent of user agreement on the selected priorities, the risk analysis methodology, and other related matters should be described in detail adequate to a full understanding of the relative priorities to be observed in recovery of operations and of the rationale used to establish those priorities. In many organizations the relative criticality of the supported functions will vary with time of day, day of week and of month. Where appropriate, the description of priorities should reflect that situation.

c. Commitments to or Assumptions of Support

Recovery from any but minor, and relatively frequent, problems usually requires assistance in some form from groups beyond the immediate control of the ADP management. The assumption of such support, including letters of formal commitment by other organizations, difficulties in getting commitments, and related matters should be addressed. The list of the assumptions relative to resources might include the following:

— Availability of replacement hardware and licensed software.

— Availability of supplies possibly influenced by transportation problems in the event of a major problem.

— Utilization of another ADP facility and its formal commitment of support.

— Availability of people of all categories. (The mobility of employees after a natural disaster is frequently overestimated, particularly when that mobility requires leaving dependents in less than desirable circumstances.)

— Response of public utilities, particularly if there is a natural disaster of some kind.

— Availability of funds, including indication of gross amounts and possible sources.

3.2.4 Responsibilities

This section should document specific responsibilities as assigned by management to all activities and personnel associated with the plan, e.g., who within the data processing activity prepares the plan (by part, if appropriate), and who executes the plan. Whenever there may be a possibility of persons not knowing for what they are responsible when execution of the plan is required, the resonsibilities should be clearly specified in this section. When situations which require use of a contingency

plan occur, it is seldom during a period when the full complement of management is available. Therefore, it is critical that this section clearly delineate how the chain of command is to function when an emergency strikes. The document should explicitly indicate what emergency responsibilities are assigned and delegate the necessary authority to enable the selected individuals to carry out the assigned duties. Generally, for the emergency chain of command, it will be necessary to do this by function, e.g., shift supervisor, senior operator, rather than to named individuals. If the emergency chain of command duties are assigned in the plan to specific persons by name, and they are not present in the facility when needed, there is a distinct possibility that the entire operation may fail due to confusion about who is in charge.

3.2.5 Strategy

With relatively few exceptions, the selection of appropriate strategies should follow the risk analysis. Until the risk analysis is done, it is usually difficult to know the critical systems which must be maintained and the demands for resources which will be made to support those critical systems. Thus, it is expected that the strategy can be, at least tentatively, selected immediately after the risk analysis is complete. ADP and organizational management, as appropriate, should determine and have documented in this section the basic strategy to be followed by the ADP facility when implementing the Emergency Response, Backup Operations, and Recovery Actions (Part Three of the plan). This should be accomplished prior to planning any preparatory measures (Part Two of the plan). Information for use in developing strategy is categorized by area as follows:

a. Emergency Response

In the broadest sense, the strategy for this section is axiomatic, i.e., protect lives and property to the maximum extent possible. When developing a strategy to cover specific events, more complex actions and planning are necessary and must cover a very wide range of potential situations. To illustrate this, the strategy for coping with a severe hurricane will surely be different from that for a minor, easily controllable fire which creates smoke in the data center. In the first example, the strategy might include actions such as close the center, secure/transfer critical files, and release all personnel to allow them to assist their families. In the latter example, the strategy could be simply to execute power down procedures and evacuate all personnel to a nearby assembly point, e.g., across the street in fair weather, or to some pre-selected building in inclement weather. In any event, the strategies selected must provide a sufficient base upon which procedures can be devised which afford all personnel the immediate capability to effectively respond to emergency situations where life and property have been, or may be, threatened or harmed.

b. Backup Operations

Very few organizations will have ADP capability sufficiently dispersed geographically to permit the backup operations strategy to be unequivocally another site within the same organization. Most backup sites simply will not have sufficient equipment, personnel, supplies, etc., to sustain the complete operational requirements of another facility. The organizations which do not have redundant capabilities will be forced to develop a more detailed and difficult basic backup strategy. There are some ADP facilities which are now so highly centralized and so large that there is no other facility which can carry a considerable portion of the work representing the workload. For such activities, if it is necessary to continue providing data processing services

after sustaining significant damage, then the strategy must reflect a plan to divide the facility between two or more physical locations selected to offer reasonable probability that enough capability will survive a major loss to provide means of processing the critical workload.

Contingency plans must not be limited to plans which provide for some processing time by another facility and the acquisition of secure, remote site storage of backup files. There are other categories of resources or capabilities beyond hardware and data which require careful consideration and which, in turn, must be reflected in the overall contingency plan, e.g., people, supplies, space, transportation. Strategies for backup of each of these other resources must be not only workable in maintaining availability of each resource through the full variety of threat scenarios, but they must be mutually supportive and compatible when employed in concert in the overall contingency plan.

Much of the planning for minimizing the damage caused by loss of, or damage to, one or more critically needed resources can be done without considering all of the other resources when the scope of the damage is relatively minor and does not result in crippling of the entire facility. However, when recovery is from a major event and must be accomplished at another location with heavy dependence on backup in most resource categories, the plans must be derived from a thoroughly comprehensive strategy for recovery from these catastrophic situations. Listed, as examples to consider, are several fundamental strategies for backup of an entire facility. Strategies for operation when less than total inoperability is the problem must also be developed. One single strategy, as in the case of loss of a facility, is rarely adequate because of the need to respond to a wide variety of problem scenarios.

- Strategy 1—No Hardware Backup

Some few organizations need an ADP facility to perform their mission, but will not be seriously harmed if they are completely without it for periods of time possibly as long as two weeks. It is the nature of these operations that they are rarely, if ever, dynamic, transaction-oriented, communications dependent shops. In these few cases in which dependence on ADP is not immediate and critical, it is not unreasonable to assume that the original hardware can be repaired or replaced at the current or another location in time to avoid major loss provided only that other dependencies, such as people, data, and programs, are suitably protected through backup procedures. *Believing that backup of hardware facilities is not required is not sufficient justification for ignoring contingency planning.* Further, a sound risk analysis must support the conclusion that no backup arrangement is required.

- Strategy 2—Mutual Aid Agreements

Mutual aid agreements are at least conceptually possible when one facility can accept, without serious harm to its supported organizations, the critical work of another temporarily inoperative facility. Technically practicable transportability of work between two facilities requires that data and programs from one be acceptable to the other without other than the most modest change and, preferably, no change at all. Rehearsals are essential, and it should be recognized that they are usually costly, and generate unwelcome disruption to the shop providing backup. The rehearsals must include full operability of the critical systems of the facility which is down. These practice sessions or rehearsals must be thoroughly realistic and not, for example,

depend on the use of any resources from the inoperative facility for operation at the backup site. These are very difficult to conduct in a mutual-aid environment. To assure compatibility with the backup system, it is highly recommended that critical applications be run (daily, if necessary) at the backup facility as part of the normal job stream (with test data, files, etc.). Quite often, the site providing the backup support must drop some of its less than critical workload in order to provide the support to another facility. Also, the differences in security requirements between the sites must be considered. For example, clearance requirements at the backup site may preclude the entry of operators from the inoperative facility unless prior clearances have been obtained.

It is difficult at best to make mutual aid arrangements totally reliable. Changes in either system, (a highly likely occurrence) may instantly render the arrangement invalid. Further, management shifts may invalidate the arrangements with only short notice leaving a previously supported facility without backup.

While mutual aid agreements are conceptually feasible, they rarely, if ever, prove to be totally reliable. The penalty to the shop needing support of discovering in time of need that backup is not actually available is generally too great to warrant complete confidence in this strategy.

- Strategy 3—Contingency Centers

Contingency Centers are facilities established to provide a location into which an ADP organization which has lost its own facility can move temporarily to reestablish its operations, either completely or limited to critical systems only. These centers may be cooperatively owned by several organizations to back up the owners' facilities, or they may be established as profit-making ventures which sell rights to their use through membership fees, dues, and other charges. The evolution of these centers is still quite recent—too recent, in fact, for there to be a large body of experience to support their workability or to provide guidance as to the potential pitfalls to be avoided. Determining the feasibility of using such centers is not complex, does not seem to have hidden pitfalls, and thus should be relatively easy to do if based upon the results of the risk analysis. There are many situations in which such centers may well be the most cost-effective route to go, while there are others in which they are not an appropriate means of backup. Again, the decision must be made on a facility-by-facility basis.

Contingency Centers may be categorized as follows:

Empty Shells

Buildings with power, raised floor, and air conditioning but not data processing hardware. There are also buildings on which availability of floor space is maintained but in which there have been no preparations made such as the raised floor.

The empty shell provides a place to put replacement ADP hardware after a loss of the regular facility. A successful recovery in this contingency center environment requires consideration of a number of factors. These include:

— An adequate probability that *all* vendors of critically needed components can deliver soon enough to restore operations before unacceptable losses occur. This certainly implies several days before operation is restored.

— An adequate plan can be drawn to get back from the shell to the proper permanent site with a level of disruption that is acceptable.

— The shell is sufficiently close to the permanent site to avoid severe personnel availability problems.

— There are reasonable arrangements for limiting the number of organizations which might be concurrently in need of the shell to preclude the possibility that service to some or all is inadequate.

Equipped Contingency Centers

Complete ADP facilities including communications capabilities. These are readily usable by organizations which have compatible hardware. These equipped centers are of two basic types:

— Those which normally operate as service bureaus but which plan to discontinue the provision of these normal, service bureau services in the event that a subscriber to the contingency center has a need for all or a portion of the backup center.

— Those which are not otherwise used except to rehearse contingency plans and to assure the operation of critical functions on the backup equipment.

The planned use of the equipped contingency center requires the prior consideration of several factors, including:

— Compatibility of hardware.

— Restoration of communications. This problem can be minor when dependence is on only a few lines, but it grows rapidly with increasing communications complexity.

— The cost of initial occupancy. If the cost of "declaring an emergency" is too great, the decision to use a contingency center will be unreasonably difficult, even when using such a facility would be very convenient to recover from less than a catastrophic event.

— Security considerations. This is particularly important if several organizations are sharing the same system.

— Availability of the facility for rehearsal. This is absolutely essential.

— Probability of too many subscribers needing the facility at the same time.

— Geography. If key people have to travel far, this is a major consideration. Subsequent recovery at home is also difficult if the key people are away at a remote site.

- Strategy 4—One Facility, More Than One Location

This is achieved by having ADP in two geographically separated locations, the smallest of which is large enough to carry the critical workload for the few days needed to reestablish the inoperative facility. This strategy does not imply the installation of excess capacity great enough to carry the critical work—only the physical dispersion of the normal capability into two or more locations. The economic feasibility of this is based on the frequently confirmed assumption that, for the majority of facilities, the critical workload is less than 50% (commonly less than 20%) of the total load so that no increase in total ADP capacity is required. Hardware often does not divide

cleanly into two halves, but there is usually no requirement to have precisely 50% at each site. Any split which will suit the need for processing the critical work at either location is adequate, provided, of course, that the backup facility converts its workload to include only its critical functions.

Realization of all of the potential benefits of the two-location option requires that full capability to run critical workload exists at both locations. This generally requires availability of the full range of essential skills to be available at each site. This might, but does not necessarily, mean significant added costs. However, the feasibility of this depends heavily on the size of the operation being considered.

c. Recovery Actions

The strategy for recovery must be linked closely with that of Backup Operations as initiation of recovery actions may overlap, or be the next step after backup operations in restoring the ADP capability after partial or complete destruction of the facility, or other resources. The wide variety and scope of actions involved in recovery may dictate separating the specific recovery actions into two categories, i.e., short term and long term. Examples of common recovery strategies and scenarios are as follows:

- Repair/Restore Current Facility. ADP Facility Damaged—Backup Facilities Available for Critical Processing.

This situation which is fairly typical is heavily dependent on local conditions, e.g., how long non-critical workload can be deferred; continuing availability of equipment at the backup facility, etc. The short term strategy might be, simply, to defer non-critical work until the facility is restored, or, if possible accomplish manual processing. The long term strategy in this situation most likely would be to restore operations at the existing facility by using previously considered contractors and vendors for construction and other services needed.

- Rebuild Facility at Current Site. ADP Facility Destroyed, No Backup Facility/Hardware Available.

Hopefully, in this situation, management will have determined that there is no critical workload processed by the facility, and that short term recovery is not required, i.e., long term recovery consisting of acquiring equipment and a new facility will begin after occurrence of the disruption of service.

- Build New Facility at Different Location. ADP Facility Destroyed, Management Not Satisfied With Current Location.

If management has been actively considering the relocation of the ADP facility in the near future (1-3 years), the short term strategy may be to use a backup operations site. The long term strategy could consist of accelerating the preparation of the new facility at a different location. For this to be a viable strategy, actions for acquiring the new facility must already be well advanced.

When developing recovery strategy, careful consideration must be given to how ADP equipment will be replaced and systems transitioned in time of need. If the equipment and applications are so unique to the organization that backup is not available, and replacement during an emergency is not a viable alternative, the activity must consider transitioning at least the critical systems before the fact to equipment which would be available during a crisis. The systems so transitioned should be continually updated, tested and retained for use when needed. Thus, upon

occurrence of a disaster, the organization will at least be capable of processing critical work at a backup site. With this availability of software to process critical systems, the recovery strategy then, may be to acquire equipment compatible with that used for backup purposes. (See sec. 3.3.4, Hardware.)

3.2.6 Record of Changes

An essential element of any volatile document, such as a contingency plan, is a method of preparing, posting and recording changes to the document. Entries in this section should include change number; date; pages changed, deleted, inserted; name of person posting change; when posted; plan distribution; and other information as local conditions warrant.

3.2.7 Security of the Plan

Once documented, the plan provides a significant amount of information about the organization which, if misused, could result in considerable damage or embarrassment. Consequently, the plan should be made available to just those personnel affected by the plan. Widespread or indiscriminate dissemination to persons outside the organization should be avoided. It is recommended that a specifically designated function, e.g., security officer, control the distribution to preclude any release of the information to unauthorized persons or activities.

3.3 Part Two—Preparatory Actions

If an organization has a properly designed and documented contingency plan, and there is a loss requiring its use, this section of the contingency plan will be a key part of the document to which reference is required to reestablish the data processing operation to normal. A primary point to remember is that after the fact, it is too late to prepare for the problem, and, as noted earlier, it is very important that all needed persons know the respective roles to be played in recovery without the need to acquire and study the document.

This part of the plan, if used as described here, will usually be critical to the emergency response, backup and recovery from all but the most routine problems. This part is also the most frequently changed section of the document, because it provides the lists of detailed information and procedures which are difficult to memorize. The number of sections needed, their size, and their content will vary with the nature of the ADP facility. Shops which support a wide variety of organizational functions, which have complex procedures involving numerous people, extensive off-site record storage, and heavy dependence on communications will always have more complex requirements for information to support recovery than will less complex, but not necessarily smaller facilities.

The sections which should be considered for inclusion in Part Two of the facility's contingency plan are shown below, along with definitive information about the contents of each of the sections.

3.3.1 People

No other functional element of the many which comprise an ADP facility even approaches the flexibility, adaptability, breadth of function, and versatility provided by the people who work in it or for it. No other element is so critical to graceful recovery from damaging losses. Unfortunately, the availability, while functioning in the desired and prescribed manner, of no other functional element is as difficult to factor realistically into a contingency plan as are people. Because of this, the workable plans are those which reflect, as the primary concern, this dependence on people and which accommodate the problems they present.

Replacement hardware, backup copies of data, duplicate programs, and new floor space will usually perform about as well as the originals without need for learning or motivation. People do not.

People can be expected to innovate, perform unfamiliar tasks, work under considerable stress and work long hours if they are in a reasonably familiar environment, particularly if they are not too deprived of the creature comforts found in their normal work environments. People tend not to perform complex tasks well in a physically stressful environment unless there are also strong motivations for doing so. In a recovery operation, heavy ego involvement, belief in the inherent importance of the organization's mission, intense loyalty to particular people in the management structure, or some combination of these provide the principal motivation for people to perform well. The planners of backup and recovery must assess for each facility the degree to which it is safe to place dependence on these factors.

When extreme weather conditions, such as floods, tornadoes, and hurricanes, have created the need to invoke a contingency plan, people with dependents of whatever nature (including families, houses, cars, airplanes, and boats) are often extremely reluctant to leave them exposed and not cared for to go to a geographically remote alternate site to effect backup operations or recovery of a data processing operation. It is under stressful conditions that they often find a variety of reasons for not going, or that they do not effectively perform due to unhappiness or concern for that which they left behind. This situation must be considered a major factor in the selection of a basic philosophy for alternate site operation. Without the necessary people, there can be no recovery.

If ADP operation is at two or more locations, under common management control, as described under Strategy 4, above, then the people at sites not suffering a loss, and backing up one which did, can be in a position to drop less essential, normal tasks and pick up the critically needed functions of the site which is not operational. These people at the still-functioning, undamaged sites are in familiar surroundings and best able to carry on the critical tasks without interjection of the array of personal problems possibly facing personnel in the site which is inoperative.

If two or more sites routinely provide backup for each other during periods of equipment changeover, failure, scheduled maintenance, and other interruptions and also for purposes of rehearsal of emergency recovery, then changeover to the alternate site is relatively easy. A potential management problem does exist, however, whenever the initial or "home" site also provides operators to the backup site. In this situation, the effect of the different supervisory and reporting structure must be considered, as there is a tendency for the operators assigned to the home site to dominate the two. This may cause personality conflicts as well as a degradation of operations for both units and may well negate the objective in establishing a second site.

It is assumed that the contingency plan will be formed about several problem scenarios ranging from disruptions caused by loss of local power (even with backup) or communications, fire elsewhere in the building resulting in denial of access to the ADP facility, to major equipment failures, to intentional damage by malcontents, or to destruction of the facility by whatever cause.

This section should provide names, addresses, and telephone numbers of all people who may be required in any backup or recovery scenario. (Any organizational policies about employee privacy should be observed when compiling, distributing and protecting this list.) Prior compilation of this information is essential, as it cannot be assumed that upon occurrence of an emergency available management personnel will be sufficiently knowledgeable of the individual skills, talents and experience of assigned persons to select those needed for a particular recovery situation. (See sec. 3.2.4, Responsibilities.) Thus, it will be necessary on any list to associate people, skills and management in recovery. Alternates for persons with peculiar skills or

with skills in very short supply must be designated. Alternates should be selected, insofar as possible, from among those people not sharing a common exposure; that is, working the same shift or in the same physical area.

Every person recognized as important to the support of critically needed systems, as well as their alternates, must be aware of the dependence of the plan on them. (Critical systems should have primary and alternate personnel allocated to them.) These people must be informed of their recovery responsibilities and roles, and the roles should be rehearsed to the extent necessary. Sufficient additional training and experience must be provided to enough people to ensure that the skills necessary to recovery are available when needed.

There is absolutely no requirement to list people in order of relative importance to recovery. The list is awkward to build, difficult to use, and assumes, unreasonably, that the relative importance of these people is somehow independent of the nature of the problem.

There is a possible post-emergency problem which is, perhaps, impossible to factor into a contingency plan, but awareness of its potential is justified. It is this: people are often given far broader responsibilities during and immediately following an emergency than they normally have. Some people will perform far better than their peers and sometimes better than more senior people in the organization. In such situations it is sometimes quite difficult to get everyone back into the original and probably appropriate relationships. This potential problem should be borne in mind in considering personnel assignments in contingency plans.

3.3.2 Data

Data in any form are subject to a variety of vulnerabilities; precisely which are of significant consequence in any particular situation is a function of several factors. It is assumed here, again, that a quantitative risk analysis has preceded any effort to select plans to support backup and recovery through protection of data. It must be noted that the data protection needs of an effective, adequately comprehensive contingency plan are but rarely, if ever, satisfied solely by periodically putting copies of selected files in geographically remote vital records storage facilities.

It is very common that the total scope of a problem which creates a serious disruption of data processing is attributable solely to the accidental destruction of data for which there is no promptly available replacement copy. This stops processing until data can be recovered as certainly as a power failure would halt operations.

The dependence of many critical systems on prompt recovery of operations after data have been accidentally or intentionally modified or destroyed by unauthorized means demands greater availability than is possible if travel to and return from a vault several tens of miles away is required to regain access to those data. There are systems employed in the direct control of critical organizational activities, facilities, or operations so dynamic that even a few minutes loss of data can have serious consequences. These include air traffic control, complex facility management systems, command and control systems, airline reservation systems and others. The contingency plan must accommodate needs for prompt replacement of data.

Care must be exercised to make certain that multiple generations of backup files are taken so that the period spanned is short enough to satisfy the needs for currency (possibly in conjunction with journals of all file updates) and long enough to span the period needed for recovery. If the total period spanned by all stored copies of a file is too short, it is possible that all copies stored contain accidentally or intentionally incorporated flaws which require the availability of backup files. Thus, the storage of multiple generations is required but the periods spanned between retained versions are not necessarily equal. Again, if the rate of change is high and the dependency is great, it may be necessary to take file images as frequently as once per day or even more. However, if it is possible that a continuing flaw can

induce a problem in the data and, if it can take as long as a week to become aware of the problem, then copies should be retained for longer than a week as well. Otherwise, all backup image tapes will be flawed before the problem is recognized, thereby making recovery very difficult.

It is essential that all data on which backup and recovery are dependent be adequately recorded, maintained in a current condition, and backup copies adequately secured. Almost every facility is driven by a fairly complex array of data, including not only those data in machine-readable form but also the data normally on paper in various offices, in memoranda, and even unwritten. To the extent that recovery of operations after a loss is dependent on these data, as identified through risk analysis, they must be copied and appropriately protected. (See sec. 2.2, Critical Dependencies.)

More advanced data processing facilities have adopted the Data Dictionary concept for accountability for data, programs, and related information [15,16]. There are many different implementations, but all which have come to common usage provide a very valuable means of managing data and programs. In fact, the data dictionary is a tool specifically for data processing management, in that it reduces the amount of duplicate data and facilitates the preparation of documentation.

If a data dictionary has been fully and properly implemented and copies of it maintained in a current and physically safe condition, it can provide much data which otherwise must be derived manually and written into sections of the contingency plan.

3.3.3 Software

In a sense, software, i.e., programs, are just a special case of data. They tend to be more stable than do data, but they are sufficiently subject to change that care must be exercised that fully current versions and all necessary supporting documentation are sufficiently protected against the threats postulated in support of the risk analysis.

Application programs induce relatively peculiar vulnerabilities into the operations of an organization, e.g., fraud potential. These vulnerabilities become significantly greater with increased program size and complexity. There are many justifications for directing close management attention to the desirability of adopting one or more of the formalized programming management processes, e.g., structured programming with mandatory review processes, etc. The avoidance of and recovery from losses is only one of the many reasons for going that route.

One of the many potential benefits of these program development disciplines is the lessened dependence on the programmers who initially wrote each program. Procedures which reduce module size and complexity and enforce documentation and programming standards serve to improve maintainability and lessen dependence on specific individuals. This also, then, serves to enhance greatly the ease with which these programs can be handed off to other ADP facilities, normally or in a recovery mode, without the need for the services of the program authors.

As with conventional data, the identification and utilization of programs when a contingency plan is exercised are assisted greatly by a properly established and maintained data dictionary as mentioned above. A data dictionary system readily depicts the relationships of programs to jobs, to data, to functional areas of supported organizations, and to people and more, as may be needed.

If normal operations are in any way impeded when any author programmer is not available, this should serve as adequate indication that improved programming management is perhaps essential to a workable contingency plan.

It is very important that there be formal agreement with vendors of licensed programs, the copying of which is forbidden, to maintain the ready availability of replacement copies within a specifically stated time period. The written agreements

with the vendor(s) should be effected to allow use of the software as needed during contingencies and testing at the home site, as well as the backup location.

3.3.4 Hardware

It is frequently said that, of all of the resources on which an ADP facility has dependence, the data processing hardware is the most readily replaceable. This is only approximately correct; it is not uniformly so. Hardware of reasonably recent or current manufacture and produced in quantity usually will have a higher probability of availability to the facility needing it for replacement than will devices of which this is not true. Devices which offer potential for difficulty of replacement include these:

- Those which employ a complex array of optional features and, as such, are effectively customized. Complex communications controllers, as an example, have the potential for this problem.
- Those manufactured in small quantities, including specialized devices.
- Those which are application sensitive, such as check sorters.
- Those approaching or having reached obsolescence.
- Those manufactured by organizations no longer in existence.

The ease of replacement of hardware is usually a secondary consideration in planning recovery of critically needed systems. Relatively few organizations can wait for the period of time required for hardware replacement to bring up those systems needed earliest after a loss. Even readily available hardware requires a few days. However, some very important systems which can be delayed a few days may be heavily dependent on device replacement. Contingency plans should minimize, to the greatest feasible extent, this dependence on rapid replacement of hardware.

Operations split across two or more geographically-separated locations (Strategy 4) (see sec. 3.2.5b) so that the important systems can be run on one of two or more sites under common management will be relatively free of heavy dependence on rapid hardware replacement. Similarly, the equipped shell (Strategy 3) (see sec. 3.2.5b), if otherwise feasible and if it can provide all of the devices important to the operation, offers another option.

As with all other resource elements addressed in the contingency plan, the prompt replacement of hardware is heavily dependent on pre-loss planning. It is usually difficult for a vendor of hardware devices to make a definitive, long-term, binding commitment to replace a specific piece of equipment within a specific time period after a loss. Availability varies dramatically with the passage of time, particularly as it involves the currency of manufacture. Another major factor is the number of facilities employing the device in question and which are affected by the same source of loss. An area-wide problem might create far more severe demands on hardware vendors than does a loss limited to a single facility.

That portion of the contingency plan which involves the categorization of operations into those which will be conducted, after loss of the facility in which they are normally run on another, existing facility and those which will be deferred until the initial facility has been restored must reflect a realistic assessment of the problem of acquiring all hardware on which each such function has an absolute need. Although the hardware vendors have, for the reasons described, difficulty in making formal commitments on the availability of replacement gear, it is reasonable to expect of them candid, if informal, identification of problems in this area; problems which may not be readily apparent to contingency planners. This information should be solicited.

3.3.5 Communications

The size and complexity of a communications network supporting an ADP facility is a major factor in contingency planning. It is, however, of no greater importance than the relationship of that network to the time-critical systems. The existence of the network cannot be assumed to define a critical dependence on it—or on all of it. This dependence must be known before steps are taken to provide communications backup and recovery.

The restoration of communications, even after major disruption, is usually much quicker than the establishment of the same capability at another location. Unless a plan is in place and that plan is agreed to, including schedule, by all parties who will have a role in establishing communications at an alternate site, then recovery of communications at an alternate site within a reasonable period cannot be assumed.

There are facilities which, either fortuitously or by plan, are located so that it is feasible to have cables arriving at the facility from two different central offices of the telephone company. Even if all communications are normally with only one central office, if means are agreed to by the telephone company to route communications to the alternate central office in the event of the loss or disruption of the one normally used, significant protection against disruption of these communications will be gained. Some facilities have found it desirable and feasible to normally use leased or dial-up lines brought in through two central offices.

Restoration of lines to the original site does not accommodate the needs generated by the destruction or severe disabling of an entire facility. Under that circumstance, all communications directed to the initially-used site must be made available to the site at which the operations supported by them will be conducted.

There is generally available from common carriers a means to switch leased telephone lines under remote customer control from the initial termination to an alternate site. The switch, the control of the switch, the cost of the line to the switch and the costs of the lines to the initial location and to the alternate site are all tariffed separately. The switching of lines in this manner may be economically feasible if the number is small, the distances moderate and the dependencies great.

An alternative to the leased switch is to maintain the capability to route all communications to each of two sites, described above as Strategy 4 (see sec. 3.2.5b). With this alternate no physical changes are required and all communications supporting critical systems are directed to the remaining site.

The economic feasibility and the time dependencies must be examined carefully to determine which approach to communications backup is best for any specific facility.

3.3.6 Supplies

With the exception of a very few items which might be peculiar to a particular facility, most supplies are catalog items with reasonable availability. However, for most facilities there is a sufficiently large number and variety of such items as to make plans for stockpiling a modest quantity at another, safe location a necessary step. When every effort is being made to restore operations, even after only a relatively minor disruption, valuable time is easily lost in locating things of limited dollar value, such as tape cleaners, floor tile pullers, labels, and marking pens. This time can be saved by advance planning for the availability of such items.

Facilities which consume large quantities of paper should have available a buffer supply of a size adequate to maintain operations after a disruption of supply until a normal supply situation has been restored.

The contingency planner should bear in mind that the provision of supplies is just not a minor task to be undertaken as a part of recovery from some major disruptions such as fire, flood, civil unrest, hurricanes, tornadoes, or airplanes flying into the building. The whole scope of the catastrophe may be the loss of availability of printer paper through physical damage to a vendor's facility or anything else which

results in a business interruption there or in the means of transport from there. If the critical jobs performed by a system result in an essential paper output and if paper supply is interrupted without adequate backup, then the effective use of the system is denied as surely as if physical access to the ADP shop is denied.

Particular care must be given to the continued availability of special forms on which there may be a critical dependence. The replacement lead time on these is often measured in weeks. An adequate buffer supply should be stored off-site in a location not generally susceptible to the problems reasonably anticipated at the normal storage location.

3.3.7 Transportation

Events which disrupt transportation of people or supplies might have serious disruptive effects on the ability of data processing facilities to operate effectively. Of greater importance here, however, is the effect of loss of transport on recovery.

Area-wide power failures almost uniformly cripple all urban transport, including automobiles. Earthquakes make roads impassable. Labor difficulties can seriously impede public transport. These situations generally argue, not for plans to provide alternate means of transport, but for consideration of transport as a determinant in selecting an alternate site for conduct of critical work. The location of the backup capability should be free of whatever external problems are hampering the supported facility. Just as the supporting site should be served by another power company and another communications carrier, it should also be served by other forms of transport or not be susceptible to damage from interruption of transport.

3.3.8 Space

The provision of space into which an ADP facility can be placed after loss of an original site can be considered for two purposes, as follows:

- Space which can be used temporarily while the original site is being rehabilitated.
- Space into which the ADP operation can relocate with relative permanence.

Relocation at a temporary site usually requires installation of hardware at the temporary location and then relocation to the permanent site. This, then, implies two physical moves of processing operations with the significant disruption usually attendant on such moves. The expense is not inconsequential, particularly as it usually involves full site preparation at both locations.

A move from a damaged site to prepared or unprepared floor space after loss of a facility cannot usually be done in less than 1 week, and might take several weeks if equipment must be acquired. It should not be considered as a means of recovery of support of critically needed functions. It should only be done to restore full operation.

Recovery on the same day as the loss of capability, or within 2 to 3 days, must be at a location which is already populated with virtually all of the devices, communications, power and environmental control needed to support the critical functions.

Plans for space into which the facility can be relocated should, whenever possible, reflect future growth plans. Ideally, any move should be into a location at which the facility can stay permanently and expand as may be needed.

To the greatest extent possible, contingency plans should be drawn to minimize the possibility of temporary moves which require the diversion of key people, funds, management attention, and devices from the earliest possible recovery at a permanent location. There is but little to be said for mounting a major effort to become operational in the wrong place.

3.3.9 Power and Environmental Controls

Uninterruptable Power Supply (UPS) Systems provide three potentially useful functions. They are:

- Protection against power line transients which can provoke a system interruption requiring a restart and with the potential for damage to data.
- Provide a short period, usually from 15 to 30 minutes, in which the system can be stopped gracefully following a loss of primary power from a public utility.
- Provide a short period following a primary power failure during which time a standby generator can be brought into operation to support the data processing operation or at least the critical functions.

There are installed systems employing UPS for which instrumentation indicates that the UPS prevents as many as several dozen system crashes per year. This is a meaningfully large number when applied to large, real-time systems. On other systems which have little real time or online activity or very clean power, the UPS may not be justified. The determination must be made on the basis of a careful analysis of each specific facility for which it may be considered.

It must be considered in contingency planning that an unanticipated move from a complex environment providing UPS, chilled water, and 440 cycle power to a new location is not sufficiently simple to consider delaying critical systems until the move is complete. Again, as has been stated repeatedly above, provisions must be made to process critical systems on other equipment until the move is complete unless the critical load is deferrable for as long as a week. It is possible under highly fortuitous circumstances to complete a move to a new site in less than a week, but heavy dependency upon it is indeed risky.

Preparation of a backup site complete with power and all environmental systems would greatly ease the difficulty of a move to a new site, but the cost must be carefully considered. Under some circumstances where there is a plan for future growth into a site, the early preparation of the site as a contingency site can be cost justified.

It is particularly advantageous to select a backup site which is outside the "local" power grid, as this will provide alternate site processing capability when widespread local power outages occur.

In the event of partial failure of environmental controls (e.g., the air conditioning system is cooling, but at reduced capacity), it may be possible to selectively power-down less needed equipment in order to keep the computer operational. To prepare for this eventuality, a list of equipment which might be temporarily taken out of service should be prepared and maintained.

3.3.10 Documentation

This section of the plan should describe all backup documentation which is kept in the off-site facility so as to facilitate its retrieval in case of need. When preparing this section, it should be noted that one of the most critical elements of an effective data processing operation, yet, also one of the most neglected, is documentation. Without clear, concise and complete documentation, all but the simplest operations will flounder, particularly when contingency operations are effective and personnel are performing additional tasks or duties for which they are not normally responsible. For this reason, a complete set of all pertinent documentation such as Computer Operation manuals, Users manuals, Program Maintenance manuals, etc., (see FIPS Publication 38 [21], Guidelines for Documentation of Computer Programs and Automated Data Systems) should be stored in a secure off-site facility. Likewise, copies of the Contingency Plan, including equipment inventories, alternate site

agreements, etc. should be stored in a secure location which is sufficiently removed from the main facility so as not to be subject to the same major hazards, e.g., flood.

3.4 Part Three—Action Plan

This part of the plan should consist of the "what to" actions to be accomplished by those personnel or activities identified in Part One, Responsibilities. As previously indicated, and restated here for emphasis due to its importance, when an emergency strikes, the people must already know "how to" respond. Therefore, it is expected that this part of the plan will consist only of concise, short instructions of the specific actions to take as a response to each of the problem scenarios which were earlier developed (see sec. 3.2.5a-c, Strategy) for each of the three categories listed below.

3.4.1 Emergency Response

Include in this section the immediate actions to be taken in order to protect life and property and to minimize the impact of the emergency. It is recommended that a separate list of actions be developed and maintained for each of the problem scenarios. For example, different responses are required for each of the occurrences such as bomb threats, power outages, air conditioning failure, fire alarm, etc. To facilitate use of the listings, more than one copy of each will be required in addition to the master, or file copy. The number required is dependent on the size of the facility and the ease with which needed sections may be retrieved for use. In any event, it should never be necessary to search for a needed portion of the plan after an emergency requiring its use has occurred. Following is an abbreviated example of the actions which might be included as a response to a sudden power outage of unknown duration (assuming UPS is installed and operative):

- Initiate power down procedures
- Notify key personnel
- Notify customers of disruption of service

The detailed instructions on how to accomplish the tasks listed above, and others as applicable to the facility should be located in Part Two of the plan under the specific categories of Power, People, etc.

3.4.2 Backup Operations

In this section, describe what must be done to initiate and effect backup operations, separately for each of the scenarios developed. For example, if the scenario is: major power outage of expected 3-day duration; backup operations at primary alternate facility necessary, the list of actions to take might include, but not be limited to:

- Notify alternate facility
- Notify backup team
- Notify customers of disruption of service
- Arrange transportation
- Retrieve backup supplies
- Assemble copies of software, data, documentation, etc.

Any "how to" instructions for each of the above areas should have been included in Part Two of the plan under preparatory actions.

3.4.3 Recovery Actions

As in the two preceding sections, the instructions in this section should be limited to describing what to do in effecting recovery from the situations documented in the

problem scenarios. For example, if the scenario is: the ADP facility has been damaged, some equipment destroyed, but critical applications may continue to be processed. The action list in this case might reflect items such as:

- Perform survey to determine specific facility, hardware or data damage and losses.
- Retrieve backup files, as necessary. (Consider the possibility that if the primary file is destroyed and if the only backup copy of the file is retrieved from the off-site storage, no further backup is available until the backup file is copied.)
- Submit equipment order to vendor. (Equipment data should be available from Part Two of the plan.)

4. TESTING

One of the more important aspects of successful contingency planning is the continual testing and evaluation of the plan itself. Quite simply, a plan which has not been tested cannot be assumed to work. Likewise, a plan documented, tested once and then filed away to await the day of need provides no more than a false sense of security. Data processing operations are, historically, volatile in nature, resulting in frequent changes to equipment, programs, documentation, customer requirements, and often even in the way daily business is conducted. These actions make it critical to consider the plan in the same context, i.e., one in which frequent changes occur. A plan quite adequate today may be woefully unsatisfactory 2 months, or less, from now. Suffice to say, that if the ADP contingency plan is not subjected to continual and rigorous management review as well as to in depth testing on a scheduled basis it will fail when needed.

4.1 Test Plans

The devising of test plans which adequately and reliably exercise the contingency plan themselves require considerable skill and great care so as to meet the objective of providing tests which are entirely realistic while still being economically feasible.

Care must be taken to see that the tests involve the most important systems to be supported in the contingency environment. The testing of the simpler jobs may be desirable initially, but such tests do not provide adequate assurance that the critical jobs will run.

4.2 Conducting Testing

A good argument can be presented that the only method to test a contingency plan completely is to actually cease or otherwise disrupt operations at the facility for which the plan has been prepared; however, this is seldom practical, and quite possibly could, in itself, create actual losses in capability. It is generally only necessary to assume that operations at the home site are disrupted or otherwise not available. For example, it is not essential to have an actual fire in order to test the emergency evacuation procedures. What is needed is an understanding with the fire department and documentation of the specific test procedures to follow in simulating the fire and emergency condition. Likewise, to test backup operations at an alternate site, it is not mandatory to cease operations at the home site, but rather to gather copies of all needed data and other information required to actually begin operations at the alternate facility. In situations such as this, the test most heavily inconveniences the supporting (alternate) facility which is assumed to be unharmed in the simulated catastrophe, or disruption of service.

4.3 Test Plan Documentation

The test plans should form a formal part of the contingency plan documentation and be as fully subject to the review and approval process as the other sections of the plan.

5. REFERENCES AND ADDITIONAL READINGS

[1] Becker, Robert S., The Data Processing Security Game: Safeguarding Against the Real Dangers of Computer Abuse. Pergamon Press, Inc., Elmsford, NY (1977) ISBN: 0-08-021790-7.

[2] Broadbent, D., Contingency Planning, The National Computing Centre, Oxford Road, Manchester, United Kingdom (1979).

[3] Browne, Peter S., Security: Checklist for Computer Center Self Audits, AFIPS Press, Montvale, NJ 07645 (1979). (Order from AFIPS, 1815 N. Lynn Street, Suite 800, Arlington, VA 22209.)

[4] Canning, R., Computer Security: Backup and Recovery Methods. EDP Analyzer. 10(1); (1972 January).

[5] Carroll, John M., Computer Security, Security World Publishing Co., Inc., Los Angeles, CA (1977) ISBN: 0-913708-28-3.

[6] Computer Control & Audit, Institute of Internal Auditors, Altamonte Springs, FL (1978).

[7] Courtney, Robert H., Jr. and Orceyre, Michael J., Considerations in the Selection of Security Measures. Washington, DC: GPO; 1978 June; NBSSP 500-33. Available from: GPO, Washington, DC; SN 003-003-01946-1.

[8] Courtney, Robert H., Jr., Security Risk Assessment in Electronic Data Processing Systems, Technical Report 21.700, IBM Corporation, Kingston, NY 12401.

[9] Checklists and Guidelines for Reviewing Computer Security and Installations, Management Advisory Publications, P.O. Box 151, 44 Washington Street, Wellesly Hills, MA 02181 (1975).

[10] Data Security and Data Processing, Vol. 1-6, (G320-1371, 1372, 1373, 1374, 1375, 1376) IBM Corporation, White Plains, NY 10604 (1974).

[11] Data Security Controls and Procedures—A Philosophy for DP Installations, G320-5649-00, IBM Corporation, White Plains, NY 10604 (1976).

[12] Disaster Preparedness, Office of Emergency Preparedness Report to Congress, Stock Number 4102-0006, Government Printing Office, Washington, DC (1972).

[13] Hoyt, Douglas B., Ed., Computer Security Handbook, McMillan Information, New York (1973).

[14] International Business Machines Corporation (IBM). An Executive's Guide to Data Security—A Translation from an IBM Svenska AB Publication. IBM World Trade Corporation, New York, NY (1975 October).

[15] Institute for Computer Sciences and Technology, A Survey of Eleven Government-Developed Data Element Dictionary/ Directory Systems. Washington, DC: GPO; 1977 August; NBSSP 500-16. Available from: GPO, Washington, DC; SN 003-003-01817-1.

[16] Leong-Hong, Belkis, and Marron, Beatrice, Technical Profile of Seven Data Element Dictionary/Directory Systems. Washington, DC: GPO; 1977 February; NBSSP 500-3. Available from: GPO, Washington, DC; SN 003-003-01725-6.

[17] Martin, James, Security, Accuracy and Privacy in Computer Systems, Prentice-Hall, Inc., Englewood Cliffs, NJ (1973).

[18] Martincic, J. A., A Disaster Recovery Plan, Journal of System Management, 1976 February.

[19] National Bureau of Standards Building Science Series 46, Building Practices for Disaster Mitigation (1973 February).

[20] NBS. Guidelines for Automatic Data Processing Physical Security and Risk Management. Washington, DC: GPO; 1974 June; FIPS 31. Available from: NTIS, Springfield, VA; FIPS-PUB-31.

[21] NBS. Guidelines for Documentation of Computer Programs and Automated Data Systems. Washington, DC: GPO; 1976 February 15; FIPS 38. Available from: NTIS, Springfield, VA; FIPS-PUB-38.

[22] NBS. Guidelines for Automated Data Processing Risk Analysis. Washington, DC: GPO; 1979 August 1; FIPS 65. Available from: NTIS, Springfield, VA; FIPS-PUB-65.

[23] Nielson, N. R., Ruder, B., Madden, J. D. and Wong, P. J., Computer System Integrity, SRI International, Menlo Park, CA (1978).

[24] Parker, Donn B., Crime by Computer, Charles Scribner's Sons, NY (1976).

[25] Pritchard, J. A. T., Contingency Planning, The National Computing Centre (U.K.), Computer Security Services (1976).

[26] Report to the Congress of the United States, U.S. General Accounting Office, Most Federal Agencies Have Done Little for ADP Disasters (AFMD-81-16), 1980 December 18.

[27] Schabeck, T. A., Emergency Planning Guide for Data Processing Centers, Assets Protection Journal, 500 Sutter Street, Suite 503, San Francisco, CA 94102 (1979).

[28] Wong, K. K., Computer Security Risk Analysis and Control, Hayden Book Co., Inc., Rochelle Park, NJ (1977).

6. APPENDIX ONE

CONTINGENCY PLAN OUTLINE

Part One—Preliminary Planning

1.1 Purpose

- Reason for plan
- Objectives

1.2 Scope

- Applicability of plan
  - Data center 1
  - Data center 2

1.3 Assumptions

- Events included
- Events excluded
- Priorities
- Support commitments

1.4 Responsibilities

- Plan preparation/maintenance
- Emergency chain of command
- Operations supervisor
- Shift supervisor

1.5 Strategy

- Emergency response
- Backup operations
- Recovery

1.6 Record of Changes

- Change sheet
- Plan distribution

Part Two—Preparatory Actions

2.1 People

- Complete listing of assigned personnel with address, phone number, etc.
- Emergency notification roster(s)
- Team composition
  - Recovery Team A
  - Recovery Team B

2.2 Data

- On-site inventory
- Off-site inventory
  - How/when rotated
- Critical files needed for backup site processing

2.3 Software

- System
  - On-site inventory
  - Off-site inventory
    - How/when updated
- Applications
  - On-site inventory
  - Off-site inventory
    - How/when rotated

2.4 Hardware

- Inventory list reflecting vendor, name, address, etc.
- Emergency acquisition agreement
- Sample order forms, etc.

2.5 Communications

- Current on-site requirements
- Requirements for backup site(s)

2.6 Supplies

- List of critical supply items with all necessary information (e.g., stock numbers for ordering)
- List of vendors who provide supplies
- List/location of supplies needed for backup site processing

2.7 Transportation

- Requirements for recovery operations/backup site(s)
- Procedures for obtaining emergency transportation

2.8 Space

- Current site requirements (lay-out of facility)
- Backup site space available, by site

2.9 Power and Environment

- Current site requirements
- Backup site requirements

2.10 Documentation

- On-site inventory
- Off-site inventory
  - How/when updated
- List/location of critical documentation needed for backup site processing

2.11 Other

- Alternate site agreements
- Contracts

2.12 Test Plans

- Plan A
- Plan B

Part Three—Action Plan

3.1 Emergency Response

Scenario 1
Scenario 2
Scenario n

3.2 Backup Operations

Scenario 1
Scenario 2
Scenario n

3.3 Recovery Actions

Scenario 1
Scenario 2
Scenario n

NOTE: The exclusion of any item in the examples above does not imply that further entries may not be required for any facility. The purpose of the example entries is to suggest, generally, possible relevant entries for each facility's contingency plan. Most planners will undoubtedly discover that in order to provide complete coverage, further expansion of the outline will be necessary.

7. GLOSSARY

Backup Operation

A method of operation to complete essential tasks (as identified by the risk analysis) subsequent to disruption of the ADP facility and continuing until the facility is sufficiently restored.

Contingency Plans

Plans for emergency response, backup operations and post-disaster recovery maintained by an ADP facility as a part of its security program.

Emergency Response

A response to emergencies such as fire, flood, civil commotion, natural disasters, bomb threats, etc., in order to protect lives, limit the damage to property and minimize the impact on ADP operations.

Recovery

The restoration of the ADP facility or other related assets following physical destruction or major damage.

Risk Analysis

An analysis of system assets and vulnerabilities to establish an expected loss from certain events based on estimated probabilities of the occurrence of those events.

NBS TECHNICAL PUBLICATIONS

PERIODICALS

JOURNAL OF RESEARCH—The Journal of Research of the National Bureau of Standards reports NBS research and development in those disciplines of the physical and engineering sciences in which the Bureau is active. These include physics, chemistry, engineering, mathematics, and computer sciences. Papers cover a broad range of subjects, with major emphasis on measurement methodology and the basic technology underlying standardization. Also included from time to time are survey articles on topics closely related to the Bureau's technical and scientific programs. As a special service to subscribers each issue contains complete citations to all recent Bureau publications in both NBS and non-NBS media. Issued six times a year. Annual subscription: domestic $13; foreign $16.25. Single copy, $3 domestic; $3.75 foreign.

NOTE: The Journal was formerly published in two sections: Section A "Physics and Chemistry" and Section B "Mathematical Sciences."

DIMENSIONS/NBS—This monthly magazine is published to inform scientists, engineers, business and industry leaders, teachers, students, and consumers of the latest advances in science and technology, with primary emphasis on work at NBS. The magazine highlights and reviews such issues as energy research, fire protection, building technology, metric conversion, pollution abatement, health and safety, and consumer product performance. In addition, it reports the results of Bureau programs in measurement standards and techniques, properties of matter and materials, engineering standards and services, instrumentation, and automatic data processing. Annual subscription: domestic $11; foreign $13.75.

NONPERIODICALS

Monographs—Major contributions to the technical literature on various subjects related to the Bureau's scientific and technical activities.

Handbooks—Recommended codes of engineering and industrial practice (including safety codes) developed in cooperation with interested industries, professional organizations, and regulatory bodies.

Special Publications—Include proceedings of conferences sponsored by NBS, NBS annual reports, and other special publications appropriate to this grouping such as wall charts, pocket cards, and bibliographies.

Applied Mathematics Series—Mathematical tables, manuals, and studies of special interest to physicists, engineers, chemists, biologists, mathematicians, computer programmers, and others engaged in scientific and technical work.

National Standard Reference Data Series—Provides quantitative data on the physical and chemical properties of materials, compiled from the world's literature and critically evaluated. Developed under a worldwide program coordinated by NBS under the authority of the National Standard Data Act (Public Law 90-396).

NOTE: The principal publication outlet for the foregoing data is the Journal of Physical and Chemical Reference Data (JPCRD) published quarterly for NBS by the American Chemical Society (ACS) and the American Institute of Physics (AIP). Subscriptions, reprints, and supplements available from ACS, 1155 Sixteenth St., NW, Washington, DC 20056.

Building Science Series—Disseminates technical information developed at the Bureau on building materials, components, systems, and whole structures. The series presents research results, test methods, and performance criteria related to the structural and environmental functions and the durability and safety characteristics of building elements and systems.

Technical Notes—Studies or reports which are complete in themselves but restrictive in their treatment of a subject. Analogous to monographs but not so comprehensive in scope or definitive in treatment of the subject area. Often serve as a vehicle for final reports of work performed at NBS under the sponsorship of other government agencies.

Voluntary Product Standards—Developed under procedures published by the Department of Commerce in Part 10, Title 15, of the Code of Federal Regulations. The standards establish nationally recognized requirements for products, and provide all concerned interests with a basis for common understanding of the characteristics of the products. NBS administers this program as a supplement to the activities of the private sector standardizing organizations.

Consumer Information Series—Practical information, based on NBS research and experience, covering areas of interest to the consumer. Easily understandable language and illustrations provide useful background knowledge for shopping in today's technological marketplace.

Order the **above** *NBS publications from: Superintendent of Documents, Government Printing Office, Washington, DC 20402.*

Order the **following** *NBS publications—FIPS and NBSIR's—from the National Technical Information Services, Springfield, VA 22161.*

Federal Information Processing Standards Publications (FIPS PUB)—Publications in this series collectively constitute the Federal Information Processing Standards Register. The Register serves as the official source of information in the Federal Government regarding standards issued by NBS pursuant to the Federal Property and Administrative Services Act of 1949 as amended, Public Law 89-306 (79 Stat. 1127), and as implemented by Executive Order 11717 (38 FR 12315, dated May 11, 1973) and Part 6 of Title 15 CFR (Code of Federal Regulations).

NBS Interagency Reports (NBSIR)—A special series of interim or final reports on work performed by NBS for outside sponsors (both government and non-government). In general, initial distribution is handled by the sponsor; public distribution is by the National Technical Information Services, Springfield, VA 22161, in paper copy or microfiche form.

U.S. DEPARTMENT OF COMMERCE
National Technical Information Service
5285 Port Royal Road
Springfield, Virginia 22161

OFFICIAL BUSINESS

POSTAGE AND FEES PAID
U.S. DEPARTMENT OF COMMERCE
COM-211

3rd Class Bulk Rate

U.S.MAIL